Raheem Reed
Colin Wilde
Benjamin Hobbs
Natasha Siramarco

Systems Selection

Review the project scenario and guidelines. Meet as a team and decide what systems, platforms, or tools you'll be using this project. Each should represent a clear, logical solution to a problem the client company is facing.

Create a high-level list of systems, platforms, or tools you're going to implement for your client. For each, explain:

Windows 10 Pro VM

Backup and Restoration System - Bacula

1. How does it fit into your scenario's requirements?
    - Bacula Enterprise is ideal to protect our client's most valuable asset: their intellectual property and data.
        i. Currently used by NASA, US Navy, US Air Force (also dealing with potentially sensitive information about space and space travel)
        ii. Information Security is a high priority
        iii. Physical, and Virtual options available without using cloud
            1. Multiple OS support
            2. Multiple Hypervisors supported (Proxmox, KVM, Hyper-V, Xen, VMware, RHV, Nutanix, Azure, Oracle)
        iv. Can scale very well (and easily)
    - What problem or pain point does it solve? In other words, what value does this add to your client?
        i. Minimizes downtime in event of failure
        ii. Highly reliable backup solution that supports different backup strategies (full, diff, increm, on-prem, offsite, etc)
2. Minimum Viable Product (MVP) definition.
    - What is the minimum required for you to present on your demo day?
        i. Demonstrate the restore point
            1. Have a restore point and show a file
            2. Delete the file
            3. Restore the restore point

4. Show the file is back

Email Client- Claws Mail and ubuntu server

3. How does it fit into your scenario's requirements?
    - For the client to have a desktop email client for the users on all accounts as part of their expansion.
    - Have a shared file for the users to maintain their data up to date
4. What problem or pain point does it solve? In other words, what value does this add to your client?
    - This will allow for both technical and non-technical users who are located on and off premise to have an email system which can be linked with their personal email as well.
    - This allows for ease of use of files and folders to be connected under the same server to allow all users to have business continuity.
5. Minimum Viable Product (MVP) definition.
    - What is the minimum required for you to present on your demo day?
        i. To demonstrate that the email client is connected to the users personal email account
        ii. Also show that the shared filed had been enabled via cross platform

Remote Connection- TeamViewer

6. How does it fit into your scenario's requirements?
    - Since technical and non technical employees would have to work while traveling,teamviewer is an excellent software that allows people to work remotely while on the go.
7. What problem or pain point does it solve? In other words, what value does this add to your client?
    - With TeamViewer, you can share your screen, transfer files, collaborate with others, provide technical support, or access your personal computer remotely. It offers features like file transfer, remote printing, session recording, chat functionality, and more.
8. Minimum Viable Product (MVP) definition.
    - What is the minimum required for you to present on your demo day?
        i. Demonstrate how remote connectivity will be established to the system by both your MSP and its end user.
        ii. Users must have remote access to accounts with the correct level of permissions. For access by MSP employees, Administrator access is appropriate, while it may not be for customer employees.

Automation- ninite

9. How does it fit into your scenario's requirements? This automates program installation by replacing time consuming searching by clicking each program you wish to install on one page and having all download in the background. After importing an ISO you can have dozens of programs downloaded in a matter of minutes
10. What problem or pain point does it solve? In other words, what value does this add to your client? It solves a time issue, giving the IT team more time to focus on registry edits, user account edits and other essential tasks for setting up new user PCs and accounts.
11. Minimum Viable Product (MVP) definition.
    - What is the minimum required for you to present on your demo day?
    - Not much, this is a very reliable and easy to use program.

During your pitch, your instructor will help you scope your project. Some features may become MVP and some may become stretch goals.

Once you are ready, find your instructor and pitch your solution ideas.

Scope creep can be dangerous! Keeping your project within a predetermined scope will help the group stay on task without going off on tangents and side features.

Scenario and Requirements

Scenario

A tiny new space startup looking to build and deploy micro-satellites.

- The company has mostly been hardware and software engineers working out of a large converted garage space.

- They have received some grants and some investments, and they want to expand to hire more engineers, but also a few non-technical employees such as an office manager, a media person, etc.

- Most employees will continue to work out of a central location, but both technical and non-technical users will sometimes need to travel.

- Information security is a priority: The company's only value is its intellectual property. The company is unwilling to allow these technical designs to be stored on the cloud, and does not want any of its intellectual property to leave the building (except in the form of offsite backups).

Side Notes:

Colin: Expanding company: Technical and non technical roles
Raheem: On-site and Off site (remote access)
Natasha: ***Information Security: High Priority & Intellectual Property***
Benjamin: Offsite Backup(non-cloud)

Guideline Requirements

Regardless of the specific needs of your customer, your proposal should include the following aspects and solutions:

User provisioning:

- Setup a single endpoint as you would for a new user:
    - This should include connecting the new user to whatever network or cloud resources they will use (shared folders, backup systems, email address connected to email client, etc.).
- Use any available tooling to minimize MSP labor in this process.
    - Stretch Goal: partially or fully automate this process (imagine entering only the new user’s name and email into a script and then letting the setup take care of itself).

Backup Solution:

- User endpoints will need a backup solution.
- Backups should:
    - Preserve user data.

    - Minimize user downtime in the event of system failure.

OS Diversity:

- Your project should include both Windows and Linux systems.
- What role they serve (user endpoint, server, etc.) is up to you.

Collaboration:

- Each user endpoint needs an email client:
    - Email client should be connected to the user's email.
    - Select and email provider appropriate for the company's needs:
        - Assume that the company will have its own domain name, and that the email provider will be providing the backend.
        - Create an example account on that provider for demonstration purposes.
- Shared files:
    - Users need to be able to collaborate by sharing files and documents.
    - Choose and implement an appropriate solution for this need.

Remote Access

You will need to establish technology and protocols for secure remote access.how we would establish technology and protocols for secure remote access using TeamViewer, we would follow these steps displayed:

1. Use the latest version: Ensure that both the remote and local devices have the latest version of TeamViewer installed. Regularly update the software to benefit from security patches and new features.
2. Configure security settings: Within the TeamViewer settings, enable and configure security features such as encryption, two-factor authentication (2FA), and access control. Encryption helps protect data transmitted between devices, while 2FA adds an extra layer of authentication. Access control allows you to define permissions and restrict access to specific users or devices.
3. Implement strong passwords: Enforce the use of strong, unique passwords for TeamViewer accounts. Encourage users to follow password best practices, such as using a combination of letters, numbers, and special characters, and avoiding easily guessable passwords.

4. Whitelist trusted devices: Utilize TeamViewer's whitelist feature to specify trusted devices or IP addresses that are allowed to connect remotely. This helps prevent unauthorized access from unknown or suspicious sources.
5. Limit session permissions: Configure TeamViewer to limit the permissions granted during remote sessions. Define the level of access each user or user group should have, ensuring that they only have the necessary privileges for their intended tasks.
6. Monitor and log remote sessions: Enable logging and session recording within TeamViewer to create an audit trail of remote access activities. This allows for monitoring, tracking, and detecting any suspicious behavior or unauthorized access attempts.
7. Educate users on security practices: Provide training and guidelines to users on how to use TeamViewer securely. Educate them about the importance of protecting login credentials, recognizing phishing attempts, and following security best practices when accessing systems remotely.
8. Regularly review and revoke access: Periodically review the access permissions granted to users. Remove access rights for individuals who no longer require them or when their roles change within the organization. Maintain a process for granting and revoking access as needed.
9. Network and firewall security: Ensure that the network infrastructure and firewalls in place provide adequate protection. Configure firewalls to allow only necessary traffic and consider using VPNs (Virtual Private Networks) to establish secure connections.
10. Conduct security assessments: Regularly assess the security of your remote access infrastructure, including TeamViewer. Perform vulnerability scans, penetration testing, or engage with third-party security professionals to identify and address any weaknesses.

You (the MSP) will need remote Admin/root access for management and troubleshooting.To accomplish this goal of remoting to admin/ root access for management and troubleshooting we will have to follow these steps in accordance to the task at hand:

1.Set up separate user accounts: Create separate user accounts with administrative/root privileges for remote access purposes. Avoid using the default or shared admin/root account for security reasons.

2.Strong and unique credentials: Ensure that each user account has a strong and unique password. Enforce password complexity requirements, such as a minimum length, a mix of uppercase and lowercase letters, numbers, and special characters. Consider using a password manager to securely store and generate passwords.

3.Limit remote access rights: Configure the user accounts to have the minimum required privileges for management and troubleshooting tasks. Avoid granting unnecessary permissions that could increase the risk of unauthorized access or accidental system changes.

4.Enable two-factor authentication (2FA): Enable 2FA within TeamViewer to add an extra layer of security. This can help prevent unauthorized access even if the login credentials are compromised. TeamViewer supports various 2FA methods, such as time-based one-time passwords (TOTP) or biometric authentication.

5.Restrict access through whitelisting: Use TeamViewer's whitelist feature to restrict access to specific trusted devices or IP addresses. This helps prevent unauthorized connections from unknown or suspicious sources.

6.Limit session duration and active hours: Define session time limits and active hours for remote access. This helps ensure that access is only granted during specific periods and reduces the risk of prolonged unauthorized access.

7.Monitor and log remote sessions: Enable logging and monitoring features within TeamViewer to track and record remote sessions. This helps with auditing, detecting any suspicious activities, and investigating potential security incidents.

8.Regularly review access permissions: Periodically review and reassess the remote access permissions granted to users. Remove access rights for individuals who no longer require them or when their roles change within the organization.

9.Keep TeamViewer up to date: Ensure that both the remote and local devices have the latest version of TeamViewer installed. Regularly check for updates and apply them promptly to benefit from security patches and improvements.

10.Educate users: Provide clear guidelines and training to users with remote access privileges. Educate them about best practices for secure remote access,

such as protecting login credentials, recognizing phishing attempts, and using TeamViewer responsibly.

Depending on the scenario, users may also need remote access on occasion. Evaluate the client's needs and implement an appropriate solution.For personnel that would have to use remote access occasionally we implemented a lot of steps and here they are:

1. Define a remote access policy: Create a clear policy that outlines the circumstances under which remote access is allowed, the process for requesting access, and any security requirements. This policy should be communicated to all users who may need occasional remote access.

2.User authentication: Implement a strong authentication process to verify the identity of users requesting remote access. This can include using unique IDs and passwords, multi-factor authentication, or integration with existing authentication systems.

3.Request process: Establish a formal process for users to request remote access. This can be through a ticketing system, an email request, or a specific online form. The request should include the reason for remote access, the expected duration, and any specific requirements.

4.Approval process: Assign someone within your organization to review and approve remote access requests. This person should verify the legitimacy of the request, ensure it aligns with the remote access policy, and assess any potential security risks. Only approved requests should proceed to the next step.

5.Access scheduling: Once a remote access request is approved, work with the user to schedule a specific time for the access. This helps ensure that remote sessions are planned and coordinated, reducing the risk of unauthorized or unexpected access.

6.Temporary password: To enhance security, consider generating temporary passwords for each remote access session. These passwords should be

randomly generated, unique for each session, and expire after a specific period. This helps prevent unauthorized access if the password is accidentally exposed or shared.

7.Monitoring and logging: Maintain a log of all remote access sessions, including the user, date, time, and purpose. Regularly review these logs to detect any unusual activities or potential security breaches.

8.Session termination: Ensure that remote access sessions are terminated promptly once the troubleshooting or support is complete. Encourage users to actively close the session on their end as well.

Stretch Goal: implement a solution for remotely accessing a user's system over the internet to help them troubleshoot a problem. Assume that the MSP must securely access the machine over the internet.

We will be using teamviewer as are remote access software and here are a few steps that we will use to remotely access a users systems over the internet to help them troubleshoot a problem:

1. Set up TeamViewer: Ensure that we (the Managed Service Provider) and the user have TeamViewer installed on your respective devices. We have to Make sure you are using the latest version to benefit from the latest security features and patches.

2.Establish a secure connection: The user would provide us with their TeamViewer ID and password. They can find this information within the TeamViewer software on their machine. This ID is unique to their device and allows you to connect securely.

3.Initiate the connection: Open the TeamViewer software on our device and enter the user's TeamViewer ID into the "Partner ID" field. Select the appropriate connection type (e.g., "Remote control") and click on the "Connect" button.

4.Authenticate the connection: users will be prompted to enter the user's TeamViewer password to authenticate the connection. Ensure that you securely obtain this password from the user.

5.Wait for user approval: Once we initiate the connection, the user will be prompted on their device to grant you access. They must accept the connection for it to proceed.

6.Troubleshooting and support: Once the connection is established, we will have remote control of the user's system. Then we can troubleshoot the problem, provide assistance, and perform necessary tasks as if you were physically present at their machine. Ensure that you communicate with the user throughout the process and respect their privacy.

7.Close the connection: Once the troubleshooting session is complete, close the TeamViewer connection. The user can also end the session at any time by closing the TeamViewer software or explicitly terminating the connection.

Grading

Each team member’s grade is split between their individual effort, and the project’s technical merit.

Individual effort is graded based on contributions to project deliverables, and professionalism in the presentation.

Technical merit of the project overall is evaluated according the requirements. The Project Grade is a combination of the Presentation (55%) and the Deliverables (45%)

Presentation (50%)

Components of the presentation must include:

- Team and individual introductions. (5 min)
    - One interesting/fun fact about yourself
    - Your career ambitions (where you’ve been, where you’re going, and why)
- Topical Overview (5 min)
    - As the “Problem Domain”, describe the project scenario you were assigned and the overall client requirements.
    - What solutions to the problem domain will your team be presenting today? Why did you choose these solutions?
- Present live technical demonstrations

    - All team members must present an equal share of the live technical demonstrations.
    - The presentation consists of a full provisioning demonstration of a computer system, as well as key operations.
        - OS provisioning
            - Demonstrate customization and provisioning of the required OS.
                - Skip processes that take a long time to complete. Remember, your demo time is limited.
        - System operations
            - Demonstrate user provisioning of a single end-user (non-administrator account).
            - Demonstrate how remote connectivity will be established to the system by both your MSP and its end user.
                - Users must have remote access to a accounts with the correct level of permissions. For access by MSP employees, Administrator access is appropriate, while it may not be for customer employees.
            - Demonstrate how the most important software applications and network resource features will be provisioned and supported by the MSP.
                - For example: email clients, shared network drives, cloud-based resources.
            - Demonstrate a single file or folder data backup and restoration procedure.
                - How will your MSP mitigate the risk of data loss on this new computer system? Your presentation should mention as well how you would perform a baremetal restoration if the OS were to be rendered inoperable.
        - Task automation
            - The presentation must include a live technical demonstration of a solution that automates repetitive or tedious processes.

Deliverables (50%)

- GitHub (15%)
    - An appropriately name Github “Organization”
        - Sufficient documentation in the top level README to explain to a stranger who you are, what this project was about, and how all of the material in the repo pertains to it.

            - This README should be:
                - Attractively formatted
                - Include links to relevant files and repos.
                - Include links to each of your own Github accounts AND LinkedIn accounts.
    - Separate repositories for:
        - Presentation and Project Organization materials.
        - SOPs, Topologies, and other documentation.
        - Scripts.
    - Each of these repositories should have attractive and informative `README.md`, and well labeled links to any relevant files within the repo.
- Presentation Material (5%)
    - Slide deck, as a PDF.
    - A link to the video of your presentation (when it becomes available).
- Standard Operating Procedures (SOPs), Scripts, and System Documentation (30%)
    - SOP Requirements:
        - Each SOP should include the following sections:
            - Purpose
            - Scope
            - Responsibilities
            - Prerequisites
            - Procedures
            - References
            - Definitions
            - Revision History (including who contributed to each revision)
        - For each SOP included in your MSP SOW deliverable, attribute authorship to the team member
        - SOPs can either be:
            - Worked on as google docs and submitted as PDFs
            - Worked on and submitted as Markdown files
        - SOPs should share a common format (see SOP-example-template)
        - Compose thorough SOPs for each of the following:
            - How will you backup and restore user data, critical infrastructure configurations and hosted data?
            - How will you securely dispose of sensitive data from storage media?
            - How will you perform the support engagements/interactions?
            - What troubleshooting methodology will your technicians follow during support engagements?

        - How will user or department technology purchase requests be handled?
        - How will technology needs be handled for employees being onboarded?
        - How will technology needs be handled for employees being terminated?
        - How will remote, offsite support engagements take place?
        - How will you secure Windows 10 endpoint workstations from data loss and malware threats?
        - How will you administer and support Windows systems?
        - How will your company enhance the network's usability and security?
        - How will you support company cloud services?
    - Scripts:
        - Include any Scripts written in the course of the project.
    - Systems Documentation:
        - Include in your deliverable any relevant information required for the operation of the demonstrated system.
            - Any config files which you created or customized, exported in an appropriate format (such as json)
        - Network Topology